

Masterclass: Advanced Malware Hunting and Prevention

Duration: 5 Days Course Code: AMH Delivery Method: Virtual Learning

Overview:

This course teaches the ways of identifying how malware looks like, what malicious activities you should look out for and the ways of removing it. You will also learn how to implement and manage preventive solutions both for small and medium sized for enterprises and organizations. During this course you learn what makes piece of code malicious, go through historic examples and get familiar with different kinds of malware and how to identify various cases. Once we have sufficient understanding of techniques and capabilities of malware, we will start system and network hardening – you will implement security in depth solutions, such as whitelisting or virtualization, in order to protect assets.

Target Audience:

Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security. To attend this training, you should have a good hands-on experience in administering Windows infrastructure. At least 5-8 years in the field is recommended.

Prerequisites:

- To attend this training, you should have a good hands-on experience in administering Windows infrastructure. At least 5-8 years in the field is recommended.

Testing and Certification

- After finishing the course, you will be granted a CQURE **Certificate of Completion**. Please note that after completing the course you will also be eligible to claim **CPE points!**
-

Content:

Module 1: What is malware	b) Extracting secrets	e) HTML documents
a) Malware History	c) Determining if file is packed or obfuscated	f) Living off the land binaries
b) Malware Goals	d) Fingerprinting the malware	Module 6: Advanced techniques used by malware
c) Types of Malware	e) Pattern matching using YARA	a) Malware persistence methods
d) Advanced Persistent Threats	Module 4: Behavioral malware analysis	b) Malware stealth techniques
e) Indicators of Compromise	a) Malware detonation	c) Covert channel communication
Module 2: Introduction to Malware Analysis	b) Sysinternals suite	d) Domain Generator Algorithms
a) Types of malware analysis	c) Network communication analysis	e) Anti-VM and Anti-debugging tricks
b) Goals of malware analysis	d) Monitoring system events	Module 7: Defending against malware
c) Impact analysis	e) Memory dump analysis	a) Windows security solutions
d) Containment and mitigation	f) Simulating real environment	b) Anti-Virus software
e) Incident prevention and response playbooks	Module 5: Malicious non-exe files	c) EDR software
f) Setting up sandbox environment	a) Alternative binaries	d) Principle of least privilege
g) Cloud-based malware analysis	b) PowerShell scripts	e) Application Whitelisting
Module 3: Static malware analysis	c) Office documents	f) Virtualization
a) Executable analysis	d) JScript	g) Network and domain segmentation

Additional Information:

Intense exercises:

This course is packed with unique labs exercises! To get more practice we offer three extra weeks of labs online! After the training concludes, you may practice even more and repeat to consolidate newly gained skills and knowledge.

Platform and Technical Requirements:

To participate in the course you need a Stable internet connection. For the best learning experience we also need you to have a webcam, headphones and a microphone. Open RDP port 3391 for the connection to the Lab environment is needed as well. We will setup a secure Zoom classroom for every day of the course – we will send you a safe link to join the conference by e-mail.

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A, First Floor, Office F68, Dubai, UAE